Exhibit ‘C’

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO

MELODY JOY CANTU AND DR. RODRIGO CANTU,

Plaintiffs,

v.

DR. SANDRA GUERRA and DIGITAL FORENSICS CORPORATION, LLC,

Defendants.

5:20-CV-0746 JKP – HJB

PLAINTIFFS' PROPOSED SUPPLEMENTAL MOTION FOR SUMMARY JUDGMENT

Table of Contents

Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu file this Supplemental Motion for Summary Judgment, as newly produced evidence from Defendants of their phishing campaign and use of malicious scripts against Plaintiffs warrants relief.

Background

In their Amended Complaint, Plaintiffs assert claims against Defendants under the Federal Computer Fraud and Abuse Act, Texas's statutes covering unauthorized access to computers, as well as the Texas state tort of malicious prosecution.[1] Defendants jointly conspired to engage in the malicious prosecution of Defendant Melody Joy Cantu as well as the stalking and harassment of both Plaintiffs through a campaign of hacking, phishing, and surveillance in violation of federal and Texas law.[2]

Defendant Dr. Sandra Guerra hired Defendant Digital Forensics Corporation ("DFC") to hack, investigate and surveil Plaintiffs.[3] As part of this conspiracy, DFC produced a "Phase I"

---

[1] (1) Unauthorized Access to a Protected Computer 18 U.S.C. 1030(a)(2)(c); (2) Unauthorized Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(A); (3) Unauthorized Access to a Protected Computer Recklessly Causing Damage 18 U.S.C. 1030(a)(5)(B); (4) Unauthorized Access to a Protected Computer Causing Damage And Loss 18 U.S.C. 1030(a)(5)(C); (5) Conspiracy to Commit Unauthorized Access to a Protected Computer 18 U.S.C. 1030(a)(2)(c) & 1030(b); (6) Conspiracy To Commit Unauthorized Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(A) & 1030(b); (7) Conspiracy To Commit Reckless Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(B) & 1030(b); (8) Conspiracy to Commit Unauthorized Access to a Protected Computer Causing Damage And Loss 18 U.S.C. 1030(a)(5)(C) & 1030(b); (9) Knowingly Accessing Without Effective Consent a Computer, Computer Network, Or Computer System Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.02(a); (10) Knowingly Accessing a Computer, Computer Network, or Computer System With The Intent to Defraud, or Harm Another or Alter, Damage, or Delete Property Without Effective Consent Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.02(b-1); (11) Electronic Access Interference Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.022; and (13) Malicious Prosecution.

[2] *See* Dkt. 6, Am. Compl.

[3] *See e.g.* Dkt. 110, Ex. A, BATES#: D 000060-61 (Aff. of Dr. Guerra stating she has retained DFC.

report for Defendant Dr. Guerra.[4] The Phase I report contained a sample affidavit written by DFC for use by Dr. Guerra to submit as part of a police report. DFC required the filing of the police report in order to do further work for Defendant and generate a "Phase II" report. Defendant Dr. Guerra admitted at deposition that the affidavit she submitted to the police was substantially written by DFC and not her.[5] Moreover, the Phase I report and communications between DFC and Dr. Guerra reveal that DFC created tracking URLs deployed by Dr. Guerra against Plaintiffs.[6] DFC's belated production on November 11, 2022, was the first time that computer code containing evidence of these phishing links was produced to the Defense.[7]

The record establishes that Dr. Guerra and DFC phished Plaintiffs multiple times via text and email. DFC intentionally employed phishing links to gain access to Plaintiffs' networks.[8] The computer code produced by DFC on November 11, 2022, contains direct evidence of these phishing links as well as malicious code that allowed Defendants to improperly gain access to Plaintiffs' computer systems. During the same time period, Plaintiffs discovered that someone spliced into their cable network with a coaxial splicer.[9] At deposition, DFC's expert Shawn

---

[4] *See* Dkt. 110, Ex. B, BATES#: GUERRA 000062-87 (DFC Phase I Report.

[5] *See* Dkt. 110, Ex. C, Dep. of Dr. Guerra 45:16-46:3 (admitting she took a copy of DFC's Phase I report to the San Antonio Police Department).

[6] *See e.g.* Dkt. 110, Ex. D, BATES#: GUERRA 000340 (discussing URL tracking links deployed against Plaintiffs (marked confidential and subject to Protective Order, available for *in camera* review)).

[7] *See* Ex. A.

[8] *See* Dkt. 110, Ex. E, BATES#: D 000110-13 (phishing links sent to Plaintiffs by Dr. Guerra using fake email addresses).

[9] *See e.g.* Dkt. 110, Ex. F, MCantuProd00193-206 (service appointment scheduling and billing from Spectrum Cable to identify the issue with Plaintiff's internet network, and photos of cable splicing).

Kasal admitted that one can wiretap someone's internet connection with a coaxial cable splicer, and spoke of his knowledge of military wire-tapping surveillance techniques.[10] Furthermore, when questioned about Defendant DFC's use of a coaxial wiretap in this case, he became evasive and refused to answer questions, citing his obligations of secrecy to the military.[11]

On September 4, 2018, Defendant Dr. Guerra took the Phase I report to the San Antonio Police Department and filed a false police report against Plaintiff Melody Joy Cantu.[12] On December 21, 2018, Plaintiff Melody Joy Cantu was arrested.[13] On June 24, 2019, all charges against Plaintiff Melody Joy Cantu were dismissed by the court. [14]

On August 29, 2022, Plaintiffs filed a Motion to Compel DFC to produce withheld discovery.[15]

On November 4, 2022, Plaintiffs and Defendants entered into a Joint Advisory Agreement requiring Defendants to submit their withheld discovery to Plaintiffs.[16]

---

[10] *See* Dkt. 110, Ex. G, Dep. of S. Kasal (Jul 18, 2022) at 6:10-12:10. (discussing knowledge of military-grade splicing techniques, discussing methods of splicing, and evading further answers.

[11] *See* Dkt. 110, Ex. G, at 8:4-9:8 (refusing to answer questions, citing his obligation to the military).

[12] *See* Dkt. 110, Ex. H, GUERRA 000957-61 (police affidavit memorializing Dr. Guerra stating she hired DFC); Dkt. 110, Ex. B, at GUERRA 000086-87 (affidavit template provided by DFC to Dr. Guerra); Dkt. 110, Ex. D, at 45:16-46:3 (stating she took a copy of DFC's Phase I report to the San Antonio Police Department).

[13] *See* Dkt. 110, Ex. K, BATES#: GUERRA 000952 (docket for Plaintiff Melody Joy Cantu's criminal case in Bexar County); Dkt. 110, Ex. H, at GUERRA 000960-61 (bond report for Bexar County Criminal Case against Plaintiff Melody Joy Cantu); Dkt. 110, Ex. L, DrCantuProd#000029-30 (surety bond for criminal matter).

[14] *See* Dkt. 110, Ex. M, BATES#: GUERRA 000953-55 (order granting dismissal of criminal case against Plaintiff Melody Joy Cantu).

[15] *See* Dkt. 103.

[16] *See* Dkt. 116.

On November 11, 2022, DFC submitted deficient supplemental discovery to Plaintiffs.[17] This production includes the computer code that DFC provided to Dr. Guerra in the form of a phishing link.[18] Dr. Guerra then sent the phishing links she received from DFC to Plaintiffs as part of her campaign to surveil Plaintiffs and damage Plaintiffs' computer networks.[19]

The computer code produced by DFC is incomplete as the code indicates that the phishing protocols work with other lines of computer code that Defendants' have yet to fully produce.

The computer code includes forty-six independent uses of the word "phishing", as well as dozens of separate scripts embedded within the code.[20] Additionally, the computer code includes one-hundred-and-thirteen instances of "PeerConnection" script.[21] The computer code produced by DFC shows that DFC and Dr. Guerra conspired to deploy phishing links that contained a PeerConnection script to gain remote access to Plaintiffs' protected computer network.

On December 12, 2022, Plaintiffs sent a letter to Defendants requesting the withheld discovery materials. As of the date of this filing, the Defendants have yet to submit the requested withheld discovery.[22]

---

[17] *See* Ex. A.

[18] *See* BATES#: D 000110-13 (phishing links sent to Plaintiffs by Dr. Guerra using fake email addresses).

[19] *Id.*

[20] *See* Ex A.

[21] *Id.*

[22] *See* Ex. B.

Legal Standard

Summary judgment is appropriate if the record shows that "there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law."[23] The party seeking summary judgment has the initial burden to show the absence of a material fact.[24] A genuine issue of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the non-moving party."[25]

Once a motion for summary judgment is properly made and supported, the opposing party has the burden of showing that a genuine dispute exists.[26] Thus, to defeat a properly supported motion for summary judgment, the non-moving party "must set forth specific facts showing that there is a genuine issue for trial."[27] Whether a fact is considered to be "material" is determined by the substantive law, and "[o]nly disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment."[28] The facts shall be viewed, and all reasonable inferences drawn, in the light most favorable to the

---

[23] Fed. R. Civ. P. 56(c); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986).

[24] *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986).

[25] *Anderson*, 477 U.S. at 248.

[26] *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986).

[27] *Anderson*, 477 U.S. at 247-48 ("[T]he mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no genuine issue of material fact.").

[28] *Id.* at 248.

non-moving party.[29] Neither conclusory allegations nor unsubstantiated assertions will satisfy the nonmovant's burden."[30]

Argument

This Court should grant Plaintiffs' Supplemental Motion for Summary Judgment because no reasonable juror would find a genuine issue as to any material fact evidencing that Defendants participated in a coordinated scheme of illegal computer hacking, phishing, stalking, and surveillance against Plaintiffs, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et. seq.* ("CFAA"), the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et. seq.*, the Texas Harmful Access by Computer Act §143.001 ("HACA"), Texas Penal Code § 33.02(b-1) (1), and the Texas torts of malicious prosecution and intentional infliction of emotional distress. Furthermore, no reasonable juror could find a genuine issue as to any material fact evidencing that Defendants coordinated to maliciously prosecute Plaintiff Melody Joy Cantu and violate the Texas tort of intentional infliction of emotional distress.

I. Defendants' Deployment of Phishing Links and Malicious Scripts Against Plaintiffs Establishes Defendants' CFAA Violations

Defendants' production of their phishing links and remote access scripts used to hack and surveil Plaintiffs evidences their CFAA violations.

---

[29] *Id.* at 255.

[30] *Wallace v. Tex. Tech Univ.*, 80 F.3d 1042, 1047 (5th Cir. 1996) (quotation marks and citations omitted).

The CFAA prohibits "intentionally access[ing] a computer without authorization and thereby obtain[ing] . . . information from any protected computer."[31] Such intentional access includes, but is not limited to phishing schemes that deceive users into divulging login information.[32] Additionally, the CFAA prohibits a computer accessor from exceeding their authority and using prior authorization to access another users' data to obtain or alter information in the computer that the accessor is not entitled to obtain or alter.[33]

Defendants' produced computer code includes forty-six independent instances of the term "phishing" used in association with username and password submission fields, as well as user data records. Inclusions of the term "phishing" in association with these user data points highlights Defendants' attempts to gain unauthorized and unknown access to Plaintiffs' personal data through means of deceit.

Additionally, the produced code contains one-hundred-and-thirteen instances of "PeerConnection" script. This computer script, as deployed upon Plaintiffs, allowed the Defendants to access Plaintiffs' computer networks remotely, in direct violation of the CFAA.

Further illegal conduct by Defendants can be presumed because many lines of the code that was produced on November 11, 2022, indicate that they interact with other, yet to be disclosed, computer code. While it is clear that Defendants' effectively deployed phishing links

---

[31] *See Wofse v. Horn*, 523 F. Supp. 3d 122 (D. Mass. 2021).

[32] *See United States v. Iwuanyanwu*, No. 22-1297 (1st Cir. May. 30, 2023).

[33] *See United States v. Valle*, 12 Cr. 847 (PGG) (S.D.N.Y. Jun. 30, 2014).

against Plaintiffs, it is unclear at this point to what extent Defendants' have infiltrated Plaintiffs' computer systems because the computer scripts that the phishing commands interact with have not been disclosed by the Defendants. Furthermore, the produced "PeerConnection" scripts indicate the existence of additional surveillance activities committed by Defendants that have yet to be disclosed. Regardless, the recently produced computer code is more than enough for a reasonable juror to find that Defendants unlawfully infiltrated Plaintiffs' computer networks and violated the CFAA. And the fact that the Defendants are still hiding computer code from the Plaintiffs despite multiple requests would lead any reasonable juror to conclude that the Defendants had illegally accessed Plaintiffs' computer networks in order to engage in a course of surveillance and harassment.

A. Defendant DFC's Willful Failure to Produce

Depositions reveal that Defendant DFC willfully withheld a broad swath of discovery they were obligated to produce. Only after depositions and Plaintiffs' Motions to Compel did DFC produce a small amount of material. To date, DFC has not produced their complete communications with Defendant Dr. Guerra. Moreover, the code that Defendants did produce indicates the existence of outstanding computer code that has not been produced. DFC has intentionally withheld a substantial portion of material information that Plaintiffs requested from Defendant DFC and that the discovery indicates exists.

Under the Joint Advisory, Plaintiffs sent DFC ninety-eight requests for discovery. DFC repeatedly refused to produce. DFC has only produced a small fraction of the discovery requested by Plaintiffs. Despite DFC's failure to produce, the materials that DFC has produced are more than enough to establish that there is no genuine issue as to any material fact, and that

the Defendants successfully collaborated to hack and surveil Plaintiffs' computer networks in violation of the CFAA. Moreover, the Defendants' evasiveness and refusal to produce the computer codes at issue fully further evidences their malicious hacking and infiltration of Plaintiffs' computer networks.

II. The Court Should Grant Summary Judgment as to Malicious Prosecution

The record establishes the absence of any question of material fact as to whether the elements of malicious prosecution under Texas state law have been met: (1) Defendant Dr. Guerra commenced criminal proceedings against Plaintiff Melody Joy Cantu using a form affidavit written by DFC; (2) The false charge lacked probable cause and was dismissed in Plaintiff Melody Joy Cantu's favor; (3) Defendants acted with malice as part of their campaign to stalk, harass and hack Plaintiffs.[34]

A. Dr. Guerra Admits to Taking the DFC Phase I Report to the Police

Defendant Dr. Guerra filed a false police report against Plaintiff Melody Joy Cantu at the urging of Defendant DFC. DFC expressly told Dr. Guerra that in order to obtain a Phase II report on Plaintiff Melody Joy Cantu, a police report was required.[35]

---

[34] *See e.g. Akin v. Dahl*, 661 SW 2d 917 (Tex. Sup Ct. 1983).

[35] *See* Dkt. 110, Ex. D, BATES#: D 000149 (DFC call log registering a 12-minute call with Dr. Guerra (marked confidential and subject to Protective Order, Ex. D available for *in camera* review)); Dkt. 110, Ex. B at GUERRA 000399 (Phase I report requiring Dr. Guerra to file a police report); Dkt. 110, Ex. H at GUERRA 000957-58 (police affidavit memorializing Dr. Guerra stating she hired DFC); Dkt 110, Ex. B at GUERRA 000086-87 (affidavit template provided by DFC to Dr. Guerra); Dep. of Dr. Guerra 45:16-46:3 (Dr. Guerra admits she took a copy of DFC's Phase I report to the San Antonio Police Department).

This false police report, done without probable cause, led to Plaintiff Melody Joy Cantu's arrest and prosecution.[36] Defendant Dr. Guerra admitted to the San Antonio Police Department she communicated with and hired Defendant DFC.[37]

Throughout discovery, both Defendants have been evasive and have refused to produce evidence related to their hacking, harassment, and surveillance of Plaintiffs. For instance, when asked three times at her deposition whether she had searched for responsive communications, Dr. Guerra answered "yes" and then stated that she had found none.[38] The next day Dr. Guerra's counsel produced communications between Dr. Guerra and DFC. The discovery indicates that Plaintiffs have still not received the full scope of communications between Defendants regarding their conspiracy against Plaintiffs.

Defendant Dr. Guerra's deliberate misrepresentations as to the existence of her communications with Defendant DFC in her deposition, as well as DFC's willful withholding of evidence, erases any doubt as to material facts underlying all the elements of malicious prosecution.

---

[36] *See* Dkt. 110, Ex. H, at GUERRA 000957-58 (police affidavit memorializing Dr. Guerra stating she hired DFC); Dkt. 110, Ex. C at 35:23-25 (admitting she did not know who attempted to access her account); 36:1-11 (admitting she does not know who MonkeyBar1970 is); 93:12-25 (admitting she has no evidence that her computer network was accessed without authorization), 97:1-11 (admitting her last contact with Plaintiff Melody Joy Cantu was April 1, 2018 for two-minutes outside a restaurant);Dkt. 110, Ex. J at D 000055 (Emails between DFC and Dr. Guerra discussing tracking URLs and phishing scheme).

[37] *See* Dkt. 110, Ex. H, at GUERRA 000957-58 (police affidavit memorializing Dr. Guerra stating she hired DFC); *See also* San Antonio Police bodycam footage of Dr. Guerra making her police report against Melody Joy Cantu (On file with Plaintiffs).

[38] *See* Dkt. 110, Ex. C, at 7:5-9:15 (claiming she does not recall emailing with DFC, that she had searched responsive communications, and that she found none).

Dr. Guerra has a history of misrepresentation in federal and state proceedings. Not only did Dr. Guerra unlawfully withhold information in this case and wrongfully accuse Plaintiff Melody Joy Cantu of criminal acts in order to acquire the Phase II report from DFC, but she deliberately misrepresented the truth in her lawsuit against her former employer, Humana Government Business Inc. ("Humana") in this very Court. On February 18, 2020, Dr. Guerra was fired from her role as Vice President and Chief Medical Officer at Humana for sexually harassing at least one subordinate employee at the workplace.[39] Despite admitting to her sexually lewd and unlawful conduct, and knowing that she was fired from Humana for sexual harassment of a subordinate, Dr. Guerra subsequently filed a complaint with the Texas Workforce Commission Civil Rights Division, and pursued a federal lawsuit against her former employer alleging that she was fired for racial discrimination.[40] This employment action was dismissed with prejudice.[41]

III. The Court Should Grant Summary Judgment on the CFAA Counts

The computer code recently produced by DFC proves Defendants' CFAA violations. The computer code produced shows that Defendants deployed a phishing attack that included

---

[39] *See* Declaration of Ricky Edwards, GUERRA V. HUMANA AND HUMANA GOVERNMENT BUSINESS, INC., 21-cv-00882 WDTX, Dkt. 1-4 pp. 54-55 (attached as Ex. D).

[40] *See* Texas Workforce Commission Civil Rights Division Intake Questionnaire, GUERRA V. HUMANA AND HUMANA GOVERNMENT BUSINESS, INC., 21-cv-00882 WDTX, Dkt. 1-4 pp. 18-22 (attached as Ex. E).; *See* Answer by Humana Government Business, Inc., GUERRA V. HUMANA AND HUMANA GOVERNMENT BUSINESS, INC., 21-cv-00882 WDTX, Dkt. 2 (attached as Ex. F).

[41] *See* Order of Dismissal with Prejudice, GUERRA V. HUMANA AND HUMANA GOVERNMENT BUSINESS, INC., 21-cv-00882 WDTX, Dkt. 12 (attached as Ex. G).

malicious code that allowed Defendants to gain remote access to Plaintiffs' protected computer networks. This new discovery, though incomplete, shows that there is no genuine issue as to any material fact and supports the proposition that Plaintiffs are entitled to judgment as a matter of law.

A. Unauthorized Access under 18 U.S.C. §1030 (a)(2)(C)

Plaintiffs' computers are used in interstate commerce and are "protected computers" as the term is used in 18 U.S.C. §1030 (e)(2)(B). Plaintiffs maintained and secured their computers by reasonable means, and never authorized Defendants to access them. Defendants Dr. Guerra and DFC conspired together to intentionally access Plaintiff Melody Joy Cantu's protected computers without authorization.[42] The computer code produced by DFC contains numerous phishing and remote connection scripts that were deployed against Plaintiffs and allowed Defendants to unlawfully access Plaintiffs' protected computers.[43]

Defendants used phishing links to gain unauthorized access to Plaintiffs' protected computers.[44] Phishing is a violation of Texas criminal law.[45]

---

[42] *See* Dkt. 110, Ex. N at BATES#: D 000031-32 (communications between Dr. Guerra and DFC including Plaintiff Dr. Cantu's PII (marked confidential and subject to Protective Order, Ex. N available for *in camera* review); Dkt. 110, Ex. N, at D 000034-54 (DFC sends background check on Plaintiff Melody Joy Cantu to Dr. Guerra); Dkt. 110, Ex. A, at D 000060-61 (Retainer agreement between Dr. Guerra and DFC).

[43] *See* Ex. A.

[44] *See* Dkt. 110, Ex. H, at D 000110-D 000113 (emails in which Dr. Sandra forwards to DFC emails from fake email addresses she phished Plaintiffs with by sending URL tracking links); Dkt. 110, Ex. O at GUERRA 00339-46 (instructions from DFC directing Dr. Guerra how to deploy phishing links); Dkt. 110, Ex. B, at GUERRA 000081 (DFC Phase I report to Dr. Guerra with URL tracking link results), Dkt. 110, Ex. G at 24:4-24:10 (stating he reviewed code of the phishing links sent to Plaintiffs), 27:12-15 (conceding he reviewed raw text files), 30:19-24 (stating phishing links can be used to install malware on target networks), 35:6-22 (acknowledging he knows phishing is a crime), 37:1-7 (admitting phishing techniques employ deceptive tactics).

[45] *See* Texas Harmful Access by Computer Act §143.001 ("HACA"), Texas Penal Code § 33.02(b-1) (1).

The evidence in discovery also indicates that Defendants conspired to splice into Plaintiffs' private cable network. Plaintiffs removed a cable splicer from their Spectrum cable connection that was installed by Defendants.[46] DFC's refusal to produce complete evidence in this matter, coupled with their own expert's military-grade knowledge of cable splicing, warrants this Court finding that there is no question of material fact as to whether Defendants violated the CFAA and federal wiretap law when they unlawfully installed a cable splicer on Plaintiffs' Spectrum cable box.

As a direct result of Defendants' conduct, Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu suffered loss in expending time, money, and resources aggregating at least $5000.00 in value, to investigate the intrusion, assess the damage, and restore their systems to their prior state.[47]

B. Unauthorized Damage under 18 U.S.C. §1030 (a)(5)(A)

Defendants Dr. Guerra and DFC knowingly caused transmission of a program, information, code, or command, and intentionally caused damage without authorization. This damage includes impairment to the integrity and availability of Plaintiffs' data, programs, systems, and information on the Cantu's computers and networks resulting from computer crashes, diminished bandwidth, diminished processing time, and the deletion and alteration of

[46] Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

[47] *See* Dkt. 110, Ex. P, BATES#: Dr.CantuProd#000001-28 (receipts and invoices from Exhibit A Computer Forensics Investigation LLC to discover and assess damage to computer network); Dkt. 110, Ex Q at 000050-51 (invoices from Exhibit A Computer Forensics Investigation LLC for consultation services provided); Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

data, all caused by Defendants' phishing, wiretapping, malware, and use of malicious codes against Plaintiffs.[48]

As a direct result of Defendants' conduct, Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu suffered loss in expending time, money, and resources aggregating at least $5000.00 in value, to investigate the intrusion, assess the damage, and restore their systems to their prior state.[49]

C. Unauthorized Access and Reckless Damage Under 18 U.S.C. §1030 (a)(5)(B)

Defendants Dr. Guerra and DFC intentionally accessed Plaintiffs' protected computers without authorization and thereby recklessly impaired the integrity and availability of the Plaintiff's data, programs, systems, and information.[50] The Defendants reckless conduct caused computer crashes, diminished bandwidth, diminished processing time, and resulted in the deletion of data.[51]

---

[48] *See* Dkt. 100 Ex. G at 20:17-25 (admitting that DFC produced a package for implementation by user), 21:1-22:3 (stating that DFC's phishing methods allow DFC to access data and that he reviewed the code of the phishing links); Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

[49] *See* Dkt. 110, Ex. P at BATES#: Dr.CantuProd#000001-28 (receipts and invoices from Exhibit A Computer Forensics Investigation LLC to discover and assess damage to computer network); Dkt. 110, Ex. Q at 000050-51 (invoices from Exhibit A Computer Forensics Investigation LLC for consultation services provided); Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

[50] *See* Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer); Dkt. 110, Ex. G, at 34:22-35:5 (admitting he knows technologies that can be used to tap into systems via coaxial cable connectors); Dkt. 110, Ex. R at Dep. of Dr. Rodrigo Cantu at 18:3-16 (Plaintiff Dr. Cantu admits that he was having difficulties after DFC connected to his home internet connection.

[51] Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

As a direct result of Defendants' conduct, Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu suffered loss in expending time, money, and resources aggregating at least $5000.00 in value, to investigate the intrusion, assess the damage, and restore their systems to their prior state.[52]

D. Unauthorized Access Causing Damage and Loss under 18 U.S.C. §1030 (a)(5)(C) Exceeds the Statutory Amount of $5000

As a direct result of Defendants' conduct, Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu suffered loss in expending time, money, and resources aggregating at least $5000.00 in value, to investigate the intrusion, assess the damage, and restore their systems to their prior state.[53]

E. Defendants Conspired on all CFAA Causes of Action

This Court should grant Plaintiffs summary judgment on the conspiracy cause of action because no reasonable juror would find a genuine issue as to any material fact establishing that Defendants conspired to hack and surveil Plaintiffs' computers and networks. The evidence shows, and Defendants admit in their depositions, that Dr. Guerra paid, and DFC agreed, to a scheme of illegal computer hacking, phishing, stalking, and surveillance, in violation of the CFAA and Texas state computer law.[54] Furthermore, the computer code produced by DFC

---

[52] *See* Dkt. 110, Ex. P at BATES#: Dr.CantuProd#000001-28 (receipts and invoices from Exhibit A Computer Forensics Investigation LLC to discover and assess damage to computer network); Dkt. 110, Ex. Q at 000050-51 (invoices from Exhibit A Computer Forensics Investigation LLC for consultation services provided); Dkt. 110, Ex. F, at MCantuProd 00193-00206 (invoices from Spectrum work orders and photographs of damage caused by splicer).

[53] *Id.*

[54] *See* Dkt. 110, Ex. N, at D 000031-32 (communications between Dr. Guerra and DFC including Plaintiff Dr. Cantu's PII); *id.* at D 000034-54 (DFC sends background check on Plaintiff Melody Joy Cantu to Dr. Guerra); Dkt. 110, Ex. A, at D 000060-61 (affidavit documenting retainer agreement between Dr. Guerra and DFC); Dkt.

includes phishing and remote access scripts that Defendant's used to gain unlawful access to Plaintiffs' computer networks.

IV. The Court Should Grant Summary Judgment on the Texas State Computer Law Claims

For the same reasons argued above as to the CFAA claims, this Court should grant Plaintiffs summary judgment on the Texas state law claims. Texas State Law provides a cause of action for anyone who is injured or whose property is damaged as a result of an intentionally committed computer intrusion.[55]

Conclusion

For the reasons stated above and in Plaintiffs' initial Motion for Summary Judgment, this Court should grant summary judgment all on causes of action.[56]

110, Ex. B (Phase I report advising Dr. Guerra to file a police report); Ex. H, at GUERRA 000958 (police affidavit memorializing Dr. Guerra stating she hired DFC).

[55] Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.02(a)

[56] *See* Dkt. 110.

Brooklyn, NY
Dated: July 17, 2023

Respectfully submitted,

/s/ Michael Hassard
(NY Bar No. 5824768)
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
(718) 737 - 7264
michael@torekeland.com

/s/ Tor Ekeland
(NY Bar No. 4493631)
Pro Hac Vice
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
(718) 737 - 7264
tor@torekeland.com

Counsel for Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu

Certificate of Service

I certify that on this 17th of July 2023, a true and correct copy of the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system which will send electronic notification of such filing to the parties on record.

/s/ Michael Hassard